National Infrastructure Protection Center
CyberNotes

Issue #2001-10 ***May 21, 2001***

CyberNotes is published every two weeks by the National Infrastructure Protection Center (NIPC). Its mission is to support security and information system professionals with timely information on cyber vulnerabilities, malicious scripts, information security trends, virus information, and other critical infrastructure-related best practices.

You are encouraged to share this publication with colleagues in the information and infrastructure protection field. Electronic copies are available on the NIPC Web site at http://www.nipc.gov.

Please direct any inquiries regarding this publication to the Editor-CyberNotes, National Infrastructure Protection Center, FBI Building, Room 11719, 935 Pennsylvania Avenue, NW, Washington, DC, 20535.

Bugs, Holes & Patches

The following table provides a summary of software vulnerabilities identified between May 3 and May 18, 2001. The table provides the vendor/operating system, software name, potential vulnerability/impact, identified patches/workarounds/alerts, common name of the vulnerability, potential risk, and an indication of whether attacks have utilized this vulnerability or an exploit script is known to exist. Software versions are identified if known. **This information is presented only as a summary; complete details are available from the source of the patch/workaround/alert, indicated in the footnote or linked site.** Please note that even if the method of attack has not been utilized or an exploit script is not currently widely available on the Internet, a potential vulnerability has been identified. **Updates to items appearing in previous issues of CyberNotes are listed in bold. New information contained in the update will appear as red and/or italic text.** Where applicable, the table lists a "CVE number" (in red) which corresponds to the Common Vulnerabilities and Exposures (CVE) list, a compilation of standardized names for vulnerabilities and other information security exposures.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
3Com[1]	Multiple	Office Connect DSL Router 840 4.2, 812 4.2	A remote Denial of Service vulnerability exists when connecting to the HTTP daemon and requesting a long string.	No workaround or patch available at time of publishing.	OfficeConnect HTTP Port Router Denial of Service	Low	Bug discussed in newsgroups and websites. Exploit has been published.
Apple[2]	MacOS 8.0, 8.1, 9.0	Personal Web Sharing 1.1, 1.5, 1.5.5	A Denial of Service vulnerability exists when an URL is crafted which contains excess characters.	No workaround or patch available at time of publishing.	Personal Web Sharing Remote Denial of Service	Low	Bug discussed in newsgroups and websites. Exploit has been published.

[1] Bugtraq, May 10, 2001.
[2] Bugtraq, May 10, 2001.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Cisco Systems[3]	Multiple	HSRP RFC2281	A Denial of Service vulnerability exists in the Hot Standby Routing Protocol (HSRP).	The vendor recommends deploying HSRP with IPSec. For more information see: http://www.cisco.com/networkers/nw00/pres/2402.pdf	HSRP Denial of Service	Low	Bug discussed in newsgroups and websites. Exploit script has been published.
Cisco Systems[4]	Multiple	Catalyst 2900XL Software Version 12.0 (5.2) XU	A remote Denial of Service vulnerability exists when an empty UDP packet is sent to port 161.	No workaround or patch available at time of publishing.	Catalyst 2900XL Empty UDP Denial of Service	Low	Bug discussed in newsgroups and websites. Exploit script has been published.
Cisco Systems[5]	Multiple	IOS 11.2, 11.2(4)XA, 11.2(4)XAF, 11.2BC, 11.2F, 11.2GS, 11.2P, 11.3, 11.3AA, 11.3DA, 11.3DB, 11.3HA, 11.3NA, 11.3T, 11.3WA4, 12.0, 12.0DA-12.0DC, 12.0S, 12.0T, 12.0W5, 12.0XA-12.0XJ	A remote Denial of Service vulnerability exists when an unrecognized transitive attribute in a BGP (Border Gateway Protocol) update message is received.	Upgrade available at: http://www.cisco.com	IOS BGP Transitive Attribute Denial of Service	Low/**High** **(High if DDoS best practices not in place)**	Bug discussed in newsgroups and websites.
Cisco Systems[6]	Multiple	WebNS 4.0, 4.0.1, 4.0.1B19s	A vulnerability exists in the Cisco Content Service (CSS) switch, which could allow a remote malicious user to gain access to sensitive files.	Upgrade available at: http://www.cisco.com	Content Service Switch FTP Access Control	Medium	Bug discussed in newsgroups and websites. Exploit has been published.
Comput-alynx[7]	Windows NT	CMail 2.4.9	A buffer overflow vulnerability exists which could let a remote malicious user execute arbitrary code.	No workaround or patch available at time of publishing.	Cmail Buffer Overflow	**High**	Bug discussed in newsgroups and websites. Exploit has been published.
DC Scripts[8]	Unix	DCForum 2000 1.0, 6.0	A vulnerability exists because user-supplied account information is not properly validated which could let a remote malicious user execute arbitrary commands and evaluate privileges.	Patch available at: http://www.dcscripts.com/dcforum/dcfNews/167.html	DC Scripts DCForum Remote Admin Privilege Compromise	**High**	Bug discussed in newsgroups and websites. Exploit script has been published.

[3] Bugtraq, May 3, 2001.
[4] Securiteam, May 7, 2001.
[5] Cisco Security Advisory, May 10, 2001.
[6] Cisco Security Advisory, May 17, 2001.
[7] Securiteam, May 17, 2001.
[8] qDefense Advisory Number, QDAV-5-2000-2, May 15, 2001.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Denicomp[9]	Windows 98/98/NT 3.5.1/4.0/ 2000	Winsock RSHD/NT 2.17.07 (DEC Alpha), 2.18.00 (Intel), REXECD/ NT v1.04.08 (DEC Alpha), 1.05.00 (Intel), RSHD/95 1.00.02, 2.18.03	A remote Denial of Service vulnerability exists when an abnormally long sequence of characters is sent.	No workaround or patch available at time of publishing.	Winsock rshd & rexecd Denial of Service	Low	Bug discussed in newsgroups and websites.
Drummond Miles[10]	Multiple	A1Stats 1.0	A Directory Traversal vulnerability exists due to improper validation of user-supplied input submitted as query strings to the A1Stats script, which could let a malicious user gain sensitive information.	Upgrade to the current version available at: http://www.gadnet.com/a1stats/a1s.zip	A1Stats Directory Traversal	Medium	Bug discussed in newsgroups and websites. Exploit has been published.
eEye Digital Security[11]	Windows NT 4.0/2000	Secure IIS 1.0.2	Multiple vulnerabilities exist which could expose users to security holes that SecureIIS was designed to protect.	No workaround or patch available at time of publishing.	SecureIIS Multiple Vulnerabilities	Medium/ **High**	Bug discussed in newsgroups and websites.
ElectroSoft [12]	Windows 95/98/NT 3.5.1/4.0/ 2000	Electro Comm 1.0, 2.0	A remote Denial of Service vulnerability exists when two groups of approximately 160,000 characters are submitted to the Telnet port.	No workaround or patch available at time of publishing.	ElectroComm Denial of Service	Low	Bug discussed in newsgroups and websites. Exploit script has been published.
Hughes Technol-ogies[13]	Windows 95/98/ME/ NT 4.0/2000, Unix	DSL_Vdns 1.0	A remote Denial of Service vulnerability exists when data is submitted to port 6070 and the connection is closed before the request is fulfilled.	Upgrade available at: http://lhughes.hypermart.net/vdns20.zip	DSL_Vdns Denial of Service	Low	Bug discussed in newsgroups and websites. Exploit script has been published.
IncrediMail Ltd.[14]	Windows 95/98/ME/ NT 4.0/2000	IncrediMail Build 1400185	A vulnerability exists which could let a remote malicious user create 'skin' files that will cause arbitrary files to be overwritten when the skin is loaded.	No workaround or patch available at time of publishing.	IncrediMail File Overwrite	Medium	Bug discussed in newsgroups and websites. Exploit has been published.

[9] Strumpf Noir Society Advisories, May 3, 2001.
[10] Bugtraq, May 7, 2001.
[11] Alliance Security Labs, ASLabs-2001-01, May 18, 2001.
[12] Bugtraq, May 7, 2001.
[13] Bugtraq, May 7, 2001.
[14] Bugtraq, May 11, 2001.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Jason Rahaim[15]	Windows 95/98/ME/ NT 4.0/2000	MP3Mystic 1.0, 1.0.1, 1.0.3, 1.0.4	A Directory Traversal vulnerability exists which could let a remote malicious user gain sensitive information.	Upgrade available at: http://www.i40.com/dlit.phtml?url=i40.com/mp3mystic/Files/MP3Mystic.zip	MP3Mystic Server Directory Traversal	Medium	Bug discussed in newsgroups and websites. Exploit script has been published.
Logitech[16]	Multiple	iTouch Keyboard, Cordless Freedom Pro, Navigator	A vulnerability exists with wireless mice and keyboards which could let a remote malicious user gain console access to an unauthorized system.	No workaround or patch available at time of publishing.	Logitech Wireless Peripheral Device Man in the Middle	Medium	Bug discussed in newsgroups and websites. Exploit has been published.
Maxum Rumpus[17]	MacOS 8.6, 9.1	FTP Server 1.3.2, 1.3.4, 2.0.3dev	Two vulnerabilities exist: passwords are stored in plaintext format in the prefs folder, which could let a remote malicious user access any user account on the server; and a Denial of Service vulnerability exists if you try to make a directory with a name that is 65 characters long.	No workaround or patch available at time of publishing.	FTP Server Plaintext Password and Denial of Service	Medium	Bug discussed in newsgroups and websites. Exploit has been published.
McAfee[18]	Windows 95/98/ME/ NT 4.0	Remote Desktop 32 2.1.2, 32 3.0	A remote Denial of Service vulnerability exists when a large amount of data is sent to port 5045.	Unofficial workaround (Bugtraq): Filter access to port 5045 on affected hosts. This will prevent malicious traffic from flooding the service.	McAfee Remote Desktop Denial of Service	Low	Bug discussed in newsgroups and websites. Exploit has been published.
Microsoft[19]	Windows	Internet Information Server 5.0	A remote Denial of Service vulnerability exists when a specially crafted propfind request is sent.	No workaround or patch available at time of publishing.	IIS Propfind Denial of Service	Low	Bug discussed in newsgroups and websites. Exploit script has been published.
Microsoft[20]	Windows 2000	Windows 2000 Server SP1, 2000 Server, 2000 Datacenter Server, 2000 Advanced Server	A Denial of Service vulnerability exists in the Windows 2000 Kerberos and Kerberos password services that can let a malicious user disrupt logon requests and Kerberos ticket granting.	Frequently asked questions regarding this vulnerability and the patch can be found at: http://www.microsoft.com/technet/security/bulletin/ms01-024.asp	Windows 2000 Kerberos LSA Memory Leak/ Denial of Service CVE Name: CAN-2001-0237	Low	Bug discussed in newsgroups and websites.

[15] eSecurityOnline Free Vulnerability Alert 3620, May 11, 2001.
[16] Bugtraq, May 17, 2001.
[17] Bugtraq, May 15, 2001.
[18] Bugtraq, May 16, 2001.
[19] Georgi Guninski Security Advisory #44, May 6, 2001.
[20] Microsoft Security Bulletin MS01-024, May 8, 2001.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Microsoft[21]	Windows 95/98/ME/ NT 4.0/2000, Apple MacOS 7.0-8.0, Unix	Windows Media Player 6.3, 6.4, 7	A buffer overflow vulnerability exists in the way ASX files are handled (associated video/x-ms-asf MIME type) which could let a remote malicious user execute arbitrary code.	No workaround or patch available at time of publishing.	Windows Media Player .ASX 'Version' Buffer Overflow	**High**	Bug discussed in newsgroups and websites.
Microsoft[22]	Windows 98/98/NT 4.0/20001	Internet Explorer 5.01, 5.01 SP1- SP2, 5.5, 5.5 SP1	Two vulnerabilities exist: the first vulnerability involves how digital certificates from web servers are validated, which could let a malicious user's web site masquerade as a trusted site; and the second vulnerability could enable a web page to display the URL from a different web site in the IE address bar, which could let a malicious user gain sensitive information.	Frequently asked questions regarding this vulnerability and the patch can be found at: http://www.microsoft.com/technet/security/bulletin/MS01-027.asp	IE Certificate Validation And SSL Spoofing CVE Name: CAN-2001-0338, CAN-2001-0339	Medium	Bug discussed in newsgroups and websites.
Microsoft[23]	Windows NT 4.0	Index Server 2.0	An unchecked buffer overflow vulnerability exists in the handling of user search requests, which could let a malicious user execute arbitrary code.	Frequently asked questions regarding this vulnerability and the patch can be found at: http://www.microsoft.com/technet/security/bulletin/ms01-025.asp	Index Server Buffer Overflow CVE Name: CAN-2001-0244	**High**	Bug discussed in newsgroups and websites.
Microsoft[24]	Windows NT 4.0/2000	Internet Information Server 4.0, Internet Information Services 5.0	Three security vulnerabilities exist: a vulnerability in the handling of CGI filename program requests, which could let a remote malicious user execute arbitrary commands; a vulnerability that could enable Denial of Service attacks against the FTP service due to a function that processes wiildcard sequences in FTP commands; and a flaw in the handling of FTP domain authentication that could allow a malicious user to gain access to a poorly configured network via FTP.	Frequently asked questions regarding this vulnerability and the patch can be found at: http://www.microsoft.com/technet/security/bulletin/MS01-026.asp The patch also corrects errors in three previous patches: MS00-060, MS01-014, and MS01-016 (which superseded MS01-014).	Multiple IIS Vulnerabilities CVE Name: CAN-2001-0333, CAN-2001-0334, CAN-2001-0335	Low/**High**	Bug discussed in newsgroups and websites. Exploit scripts have been published. Vulnerability has appeared in the Press and other public media.
Microsoft[25]	Windows 2000	Internet Information Server 5.0	A remote Denial of Service vulnerability exists when nonexistent files are repeatedly requested via the HTTP Lock method.	The problem has been corrected in httpext.dll v.0.9.3940.21, which is packaged with Windows 2000 Service Pack 2 available at: http://www.microsoft.com/windows2000/downloads/servicepacks/sp2/sp2lang.asp	IIS WebDav Lock Method Memory Leak Denial of Service	Low	Bug discussed in newsgroups and websites. Exploit has been published.

[21] Securiteam, May 14, 2001.
[22] Microsoft Security Bulletin, MS01-027, May 16, 2001.
[23] Microsoft Security Bulletin, MS01-025, May 10, 2001.
[24] Microsoft Security Bulletin, MS01-026, May 14, 2001.
[25] Defcom Labs Advisory, def-2001-26, May 17, 2001.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Minicom[26]	Unix	Minicom 1.82.1, 1.83.0, 1.83.1	Several format string vulnerabilities exist which could let a malicious user gain root privileges.	Temporary workaround is to remove the SGID bit from Minicom.	Minicom XModem Format String	**High**	Bug discussed in newsgroups and websites.
Multiple Vendors[27] ***RedHat & Immunix issue upgrade***[28, 29]	**Unix**	**Samba 2.0.4 -2.0.7**	**A vulnerability exists due to the insecure creation of files in the /tmp file system, which could let a malicious user alter contents of other files on the system, and potentially gain superuser privileges.**	***RedHat:*** ftp://updates.redhat.com/ ***Immunix:*** http://immunix.org/ImmunixOS/6.2/updates/	**Samba Insecure TMP file Symbolic Link**	**High**	**Bug discussed in newsgroups and websites.**
Multiple Vendors[30, 31, 32, 33]	Unix	Paul Vixie Vixie Cron 3.0pl1, 3.0.1	A vulnerability exists when a parsing error occurs after a modification operation, which could let a malicious user gain root privileges.	**SuSE:** ftp://ftp.suse.com/pub/suse/i386/update/7.1/a1/ **Debian:** http://security.debian.org/dists/stable/updates/main/ **LinuxMandrake:** ftp://sunsite.ualberta.ca/pub/Mirror/Linux/mandrake/updates/ **Progency:** http://archive.progeny.com/progeny/updates/newton/cron_3.0pl1-67_i386.deb	Vixie Cron crontab Privilege Lowering Failure	**High**	Bug discussed in newsgroups and websites. Exploit scripts have been published.
Omnicron Technol-ogies[34]	Windows 95/98/NT 4.0/2000	Omni HTTPD 2.0.8	A Denial of Service vulnerability exists when a POST request of unusual length is submitted.	No workaround or patch available at time of publishing.	OmniHTTPd Pro POST Denial of Service	Low	Bug discussed in newsgroups and websites.
OpenSSL[35]	Unix	OpenSSL versions prior to 0.9.6a	Multiple vulnerabilities exist: a vulnerability in the environment variables; several encryption flaws that allow data to be compromised; and a random number generation vulnerability which could allow a malicious user to compromise encryption.	Upgrade available at: http://www.openssl.org/source/	Multiple OpenSSL Vulnerabilities	Medium	Bug discussed in newsgroups and websites.
Oracle[36]	Windows 98se/NT 4.0/2000	Application Desktop Integrator 7.1.1.10.1	A vulnerability exists in the default configuration for plain text password storage, which could let a malicious user gain access to the APPS Schema password and potentially full access to the database.	No workaround or patch available at time of publishing.	Oracle ADI Plain Text Password Storage	Medium	Bug discussed in newsgroups and websites. Exploit has been published.

[26] Bugtraq, May 3, 2001.
[27] SecurityFocus, April 20, 2001.
[28] Red Hat, Inc. Red Hat Security Advisory, RHSA-2001:044-08, May 14, 2001.
[29] Immunix OS Security Advisory, IMNX-2001-70-019-01, May 8, 2001.
[30] Debian Security Advisory, DSA-054-1, May 7, 2001.
[31] Linux-Mandrake Security Update Advisory, MDKSA-2001:050, May 10, 2001.
[32] Progeny Service Network Security Advisory, PROGENY-SA-2001-11, May 7, 2001.
[33] SuSE Security Announcement, SuSE-SA:2001:17, May 15, 2001.
[34] Strumpf Noir Society Advisories, May 15, 2001.
[35] Bugtraq, April 24, 2001.
[36] Securiteam, May 8, 2001.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Pacific Software[37]	Windows NT 4.0	Carello 1.2.1	A vulnerability exists when a specially crafted HTTP request is sent which could let a malicious user execute arbitrary code.	Upgrade available at: http://www.carelloweb.com	Carello Shopping Cart Command Execution	**High**	Bug discussed in newsgroups and websites. Exploit has been published.
PHPProjekt Develop-ment Team[38]	Windows NT 4.0/2000, Unix	PHPProjekt 2.0, 2.0.1, 2.1	A vulnerability exists due to insufficient checking of input, which could let a remote malicious user gain access to sensitive information.	Patch available at: http://www.phprojekt.com/download/patch-2.1.tar.gz	PHPProjekt Directory Escaping		Bug discussed in newsgroups and websites. Exploit has been published.
RedHat[39]	Unix	Linux 7.0	A heap overflow vulnerability exists in the 'man' system manual pager program, which could let a malicious user execute arbitrary code.	No workaround or patch available at time of publishing.	Man -S Heap Overflow	**High**	Bug discussed in newsgroups and websites.
RimArts[40]	Windows 95/98/NT 4.0	Becky! Internet Mail 1.26.3-1.26.5, 2.0.3, 2.0.5	A buffer overflow vulnerability exists when messages are composed containing an excessive amount of characters without a carriage return, which could let a remote malicious user execute arbitrary code.	Upgrade available at: http://www.rimarts.co.jp/becky.htm	Becky! Internet Mail Buffer Overflow	**High**	Bug discussed in newsgroups and websites.
Silicon Graphics, Inc.[41]	Unix	IRIX 6.5.5-6.5.8	A buffer overflow vulnerability exists in the "rpc.espd" component of the Embedded Support Partner (ESP) subsystem, which could let a remote malicious user execute arbitrary code and gain root access.	Patch available at: ftp://patches.sgi.com/support/free/security/patches/6.5.7/patch4123.tar	IRIX rpc.espd Buffer Overflow CVE Name: CAN-2001-0331	**High**	Bug discussed in newsgroups and websites.
Spytech Software[42]	Windows 95/98/ME/ NT 4.0/2000	Spynet Chat 6.5	A remote Denial of Service vulnerability exists when 100 connection requests are received from a host within a short period of time and a message from the same host is received via the chat client.	No workaround or patch available at time of publishing.	SpyNet Chat Server Multiple Connection Denial Of Service	Low	Bug discussed in newsgroups and websites. Exploit script has been published.
Sun-Netscape Alliance[43]	Windows NT 4.0, Unix	iPlanet Web Server Enterprise Edition 4.1 sp 3-sp7	A buffer overflow vulnerability exists in the Web Publisher feature, which could let a remote malicious user gain root access.	Patch available at: http://iplanet.com/products/iplanet_web_enterprise	iPlanet Web Publisher Remote Buffer Overflow	**High**	Bug discussed in newsgroups and websites. Exploit has been published.
SuSE[44]	Unix	Matt Welsh Sgmltool 1.0.9	A vulnerability exists due to the insecure use of temporary files, which could let a malicious user overwrite the contents of target files with its own output.	Upgrade available at: ftp://ftp.suse.com/pub/suse/i386/update/	Matt Welsh sgmltool Symlink	Medium	Bug discussed in newsgroups and websites.

[37] Defcom Labs Advisory, def-2001-25, May 14, 2001.
[38] Bugtraq, May 8, 2001.
[39] Bugtraq, May 13, 2001.
[40] Bugtraq, May 14, 2001.
[41] SGI Security Advisory, 20010501-01-P, May 9, 2001.
[42] Bugtraq, May 7, 2001.
[43] Securiteam, May 17, 2001.
[44] SuSE Security Announcement, SuSE-SA:2001:16, May 4, 2001.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Symantec Corporation[45]	Windows NT 4.0	NetProwler 3.5, 3.5.1	A vulnerability exists which could let a remote malicious user defeat the password protection on the NetProwler infrastructures.	No workaround or patch available at time of publishing.	NetProwler Password Facilities Weak Design	Medium	Bug discussed in newsgroups and websites.
T. Hauck[46]	Windows 95/98/ME/ NT/4.0/ 2000	Jana Webserver 1.45, 1.46, 2.0Beta1	A Denial of Service vulnerability and a Directory Traversal vulnerability exists which could let a remote malicious user view sensitive files.	Upgrade available at: http://home.t-online.de/home/T.Hauck/Bin/Jana2E.zip	Jana Server MS-DOS Device Name Denial of Service and Hex Encoded Directory Traversal	Low	Bug discussed in newsgroups and websites. Exploit has been published.

*"Risk" is defined by CyberNotes in the following manner:

High - A high-risk vulnerability is defined as one that will allow an intruder to immediately gain privileged access (e.g., sysadmin, and root) to the system or allow an intruder to execute code or alter arbitrary system files. An example of a high-risk vulnerability is one that allows an unauthorized user to send a sequence of instructions to a machine and the machine responds with a command prompt with administrator privileges.

Medium - A medium-risk vulnerability is defined as one that will allow an intruder immediate access to a system with less than privileged access. Such a vulnerability will allow the intruder the opportunity to continue the attempt to gain privileged access. An example of a medium-risk vulnerability is a server configuration error that allows an intruder to capture the password file.

Low - A low-risk vulnerability is defined as one that will provide information to an intruder that could lead to further compromise attempts or a Denial-of-Service (DoS) attack. It should be noted that while the DoS attack is deemed low from a threat potential, the frequency of this type of attack is very high. DoS attacks against mission-critical nodes are not included in this rating and any attack of this nature should instead be considered to be a "High" threat.

Recent Exploit Scripts/Techniques

The table below contains a representative sample of exploit scripts and How to Guides, identified between May 3 and May 17, 2001, listed by date of script, script names, script description, and comments. **Items listed in boldface/red (if any) are attack scripts/techniques for which vendors, security vulnerability listservs, or Computer Emergency Response Teams (CERTs) have not published workarounds or patches, or which represent scripts that malicious users are utilizing**. During this period, 28 scripts, programs, and net-news messages containing holes or exploits were identified. *At times, scripts/techniques may contain names or content that may be considered offensive.*

Date of Script (Reverse Chronological Order)	Script Name	Script Description
May 17, 2001	ethereal-0.8.18.tar.gz	A GTK+-based network protocol analyzer, or sniffer, that lets you capture and interactively browse the contents of network frames.
May 17, 2001	execiis.c	Script that exploits the remote Microsoft IIS CGI filename decode vulnerability.

[45] Corsaire Limited Security Advisory, May 10, 2001.
[46] Securiteam, May 15, 2001.

Date of Script (Reverse Chronological Order)	Script Name	Script Description
May 17, 2001	guile.tar.gz	A toolkit that installs an encrypted backdoor on network daemons run from inetd and local suid programs. The network backdoor creates an rc4 encrypted command tunnel on a specified port and local suid backdoor spawns a rootshell when special directory conditions are met.
May 17, 2001	sa2001_02.txt	Exploit URL's included for the Microsoft IIS CGI Filename decode vulnerability.
May 17, 2001	sara-3.4.3.tar.gz	A security analysis tool based on the SATAN model.
May 17, 2001	sensedecode.tgz	Two Perl scripts which exploit the IIS URL decoding vulnerability.
May 15, 2001	dcgetadmin.pl	Perl script which exploits the DC Scripts DCForum Remote Admin Privilege Compromise vulnerability.
May 14, 2001	IIS_CGI_decode_hole.pl	Script which exploits the Microsoft IIS CGI vulnerability.
May 14, 2001	IIS_escape_test.sh	Script which exploits the Microsoft IIS CGI vulnerability.
May 14, 2001	iisex.c	Script which exploits the Microsoft IIS Multiple vulnerabilities.
May 14, 2001	iisrules.tgz	Script which exploits the Microsoft IIS Multiple vulnerabilities.
May 14, 2001	mdcrack-0.9.5.tar.gz	A brute forcer for MD5 hashes, which is capable of breaking up to 6 character passwords within hours, and 8 character passwords within two days.
May 11, 2001	ettercap-0.4.3.tar.gz	A network sniffer/interceptor/logger for switched LANs that uses ARP poisoning and the man-in-the-middle technique to sniff all the connections between two hosts.
May 11, 2001	scandisk.log	Exploit for the Jason Rahaim MP3Mystic Server Directory Traversal vulnerability.
May 9, 2001	6thSense.tgz	ATCP port scanning technique that allows you to remain completely invisible to the scanned host.
May 8, 2001	**rdC-cfingerd.c**	**Script which exploits the syslog() format string in Linux/x86.**
May 8, 2001	sara-3.4.1f.tar.gz	A security analysis tool based on the SATAN model.
May 8, 2001	**sol8_mailx.c**	**Script which exploits the /usr/bin/mailx local buffer overflow vulnerability.**
May 7, 2001	**C2900xl-crash.tgz**	**Script which exploits the Catalyst 2900XL Empty UDP Denial of Service vulnerability.**
May 7, 2001	Corntab.txt	Script which exploits the Vixie Cron crontab Privilege Lowering Failure vulnerability.
May 7, 2001	cronboom.sh	Script which exploits the Vixie Cron crontab Privilege Lowering Failure vulnerability.
May 7, 2001	**electro.zip**	**Exploit for the ElectroSoft ElectroComm Denial of Service vulnerability.**
May 7, 2001	**scs.zip**	**Exploit for the SpyNet Chat Server Multiple Connection Denial Of Service vulnerability.**
May 7, 2001	VDNS.PL	Perl script which exploits the Hughes Technologies DSL_Vdns Denial of Service vulnerability.
May 6, 2001	**vv9.pl**	**Perl script which exploits the IIS Propfind Denial of Service vulnerability.**
May 4, 2001	jill.c	Script which exploits the IIS 5.0 / Windows 2000 remote printer overflow vulnerability.
May 3, 2001	hsrp-dos.tgz	Script which exploits the Cisco HSRP Denial of Service vulnerability.
May 3, 2001	mimedefang-1.1.tar.gz	A flexible MIME e-mail scanner designed to protect Windows clients from viruses and other harmful executables.

Trends

Probes/Scans:

The CERT/CC has observed in public and private reports a recent pattern of activity surrounding probes to TCP port 10008. An artifact called the 'cheese worm' may contribute to the pattern. For more information, please see CERT® Incident Note IN-2001-05, located at: http://www.cert.org/incident_notes/IN-2001-05.html

There has been an increase in the number of scans and attacks to port 515 looking for the LPRng User-Supplied Format String vulnerability, Wu-Ftpd Remote Format String Stack Overwrite Vulnerability, ISC Bind 8 Transaction Signatures Buffer Overflow Vulnerability, and the rpc.statd Remote Format String Vulnerability.

Other:

Recent reports on IIS vulnerabilities and the large amount of NT servers being penetrated using different exploits have raised the need to tighten the security of IIS version 5.0 servers. Please see the IIS version 5.0 checklist at: http://www.microsoft.com/technet/security/iis5chk.asp.

CERT/CC has received reports of a new piece of self-propagating malicious code referred to as the sadmind/IIS worm. The worm uses two well-known vulnerabilities to compromise systems and deface web pages: A two-year-old buffer overflow vulnerability in the Solstice sadmind program; and, after successfully compromising the Solaris systems, a seven-month-old vulnerability which compromises the IIS systems. For more information, please see CERT® Advisory CA-2001-11, located at: http://www.cert.org/advisories/CA-2001-11.html.

The NIPC has received reliable information indicating ongoing attempts to disrupt web access to several sites. The activity has been seen from several networks, and consists entirely of fragmented large UDP packets directed at port 80. For more information, please see NIPC Advisory 01-012, located at: http://www.nipc.gov/warnings/advisories/2001/01-012.htm.

There has been a very significant increase in attempts to exploit known weaknesses in the lpd/LPRng and RPC daemons (ports 515 and 111) of Unix-based operating systems. For more information, please see NIPC ALERT 01-010, located at: http://www.nipc.gov/warnings/alerts/2001/01-010.htm.

The NIPC has issued an advisory concerning an unchecked buffer vulnerability in an Internet Service Application Program Interface (ISAPI) extension that could allow the compromise of an IIS 5.0 web server. For more information, please see NIPC ADVISORY 01-011, located at: http://www.nipc.gov/warnings/advisories/2001/01-011.htm.

Several Microsoft Hotfixes downloaded between April 6-20 from Microsoft's Premium Support and Gold Certifies Web sites were infected with PE_FUNLOVE.4099 (a.k.a. “the Fun Love virus”). (See the Virus Section for additional information).

Viruses

A list of high threat viruses, as reported to various anti-virus vendors and virus incident reporting organizations, has been ranked and categorized in the table below. For the purposes of collecting and collating data, infections involving multiple systems at a single location are considered a single infection. It is therefore possible that a virus has infected hundreds of machines but has only been counted once. With the number of viruses that appear each month, it is possible that a new virus will become widely distributed before the next edition of this publication. **To limit the possibility of infection, readers are reminded to update their anti-virus packages as soon as updates become available**. The table lists the viruses by ranking (number of sites affected), common virus name, type of virus code (i.e., boot, file, macro, multi-partite, script), trends (based on number of infections reported during the latest three months), and approximate date first found. During this month, a number of anti-virus vendors have included information on Trojan Horses and Worms. Following this table are descriptions of new viruses and updated versions discovered in the last two weeks. *At times, viruses may contain names or content that may be considered offensive.*

Ranking	Common Name	Type of Code	Trends	Date
1	W32/Magistr	File, Worm	Increase	March 2001
2	W32/Hybris	Worm	Slight Decrease	November 2000
3	VBS/Homepage	Script	New to Table	May 2001
4	W32/BadTrans	Worm	New to Table	April 2001
5	PE_MTX.A	File Infector, Trojan	Slight Decrease	September 2000
6	W32/Funlove	File	Increase	November 1999
7	VBS/VBSWG.Z	Script	New to Table	May 2001
8	VBS/Kakworm	Script	Decrease	December 1999
9	VBS/Loveletter	Script	Decrease	March 2000
10	W32/Bymer	Worm	Slight Decrease	October 2000

Note: Virus reporting may be weeks behind the first discovery of infection. A total of **222** distinct viruses are currently considered "in the wild" by anti-virus experts, with another **440** viruses suspected. "In the wild" viruses have been reported to anti-virus vendors by their clients and have infected user machines. The additional suspected number is derived from reports by a single source.

I-Worm.DragonBall (Internet Worm): This Internet worm spreads via e-mail messages using MS Outlook and IRC, and is written in VBS. The worm doesn't work correctly, because it contains several fatal errors. When the script is run, it creates self-copies in the system directories:

C:\Windows\Winsock.vbs
C:\Windows\Sysdir.vbs
C:\Windows\System\millioner.vbs
C:\Windows\System\DragonBall.vbs
C:\Windows\System\DragonBall.cab

Also it creates three scripts in IRC directory:

C:\mIRC\mirc.ini
C:\mIRC\script.ini
C:\mIRC\update.ini

The IRC scripts are needed for spreading via the IRC channel. As directories named "C:\Windows" and "C:\mIRC" are hard registered in worm's body, it can't execute these operations if the operation system and IRC are installed in different directories. After this, the worm changes some keys in the system registry and the WIN.INI file. This creates two keys in the registry:

[HKLM\Software\Microsoft\Windows\CurrentVersion\Run]
"winsock2.0"="C:\\Windows\\winsock.vbs"
[HKLM\Software\Microsoft\Windows\CurrentVersion\RunServices]
"sysup"="C:\\Windows\\sysdir.vbs"

and changes the value of the two keys in the WIN.INI file:

[windows]
load=C:\Windows\System\DragonBall.vbs
run=C:\Windows\System\millioner.vbs

In this way, the worm always will be run when the operation system is started. In addition to this, the worm changes another two keys in the system registry:

[HKLM\Software\Microsoft\Windows\CurrentVersion]
"RegisteredOwner"="Dragon Ball Z by YuP"
[HKCU\Software\Microsoft\Internet Explorer\Main]
"Start Page"=http://bdball.metropoli2000.net/fotos/imagenes/sagas/foto7_40.jpg

The worm contains errors, and this procedure can't work correctly, so the worm can't spread via e-mail.

JS_TODDLE.A (Alias: TODDLE.A) (JavaScript Worm): This Java Script worm propagates via Internet Relay Chat (mIRC) and requires a WScript/CScript file to be installed in order to function properly. It has no destructive payload.

VBS/Haptime-A (Visual Basic Script Worm): This is a virus that also spreads via Outlook Express 5.0. It attempts to infect files with the extensions VBS, HTML, HTM, HTT and ASP. It will also attempt to delete EXE and DLL files when the month plus the day are equal to 13 (for instance, June the 7th).

VBS/Hard-A (Visual Basic Script Worm): This virus has been reported in the wild. It is a worm that uses Outlook Express to spread. The worm arrives in an e-mail message with an attachment.
The subject of the message is "FW: Symantec Anti-Virus Warning." The body of the message contains the text:

> ----- Original Message -----
> From: warning@symantec.com
> To: supervisor@av.net; security@softtools.com; mark_fyston@storess.net; irectorcut@ufp.com; pjeterov@goldenhit.org; kim_di_yung@freeland.ch; james.heart@macrosoft.com
> Subject: FW: Symantec Anti-Virus Warning
>
> Hello,
> There is a new worm on the Net. This worm is very fast spreading and very dangerous!
> Symantec has first noticed it on April 04, 2001. The attached file is a description of the worm and how to protect your PC against it.
>
> With regards,
> F. Jones
> Symantec senior developer

The attachment filename is "www.symantec.com.vbs." If the attachment is run the worm creates an HTML file and registers it so that it is opened as a Microsoft Hypertext application file. This file is formatted in a similar way as Symantec's Anti-Virus information page, but the text describes a nonexistent worm "VBS.AmericanHistoryX_II@mm." The worm also drops a VB script file www.symantec_send.vbs into the root directory of drive C: and changes the registry key: HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run so that the file is run on the next Windows reboot. The worm sends itself to all contacts found in Outlook Express address book. On 24 November, the worm displays the message box containing the text:

> "Don't look surprised!
> It is only a warning about your stupidity
> Take care!"

VBS/LoveLet-CL (Visual Basic Script Worm): This virus is a variant of the VBS/LoveLet-A (also known as the Love Bug) e-mail-aware worm. The worm makes two copies of itself, using the filenames command.vbs and WinVXD.vbs. These files are executed each time the computer boots up. The e-mail component of the worm requires Microsoft Outlook to work. If you are using Microsoft Outlook it will try to send itself to each entry in your address book. The e-mail will have the following characteristics:

> Subject: !!!
> Body: :-) MuCuX...
> Attached file: echelon.vbs

The worm also searches all local and networked drives for files that end with the extensions VBS, VBE, JS, JSE, CSS, WSH, SCT or HTA. These files are overwritten with the worm and their extension is renamed to .VBS. The worm also overwrites any JPG or JPEG graphic files but have the extension .VBS added to the existing filename. For instance, FILE.JPG could become FILE.JPG.VBS. Any MP2 or MP3 music files are overwritten by the worm but are also copied to a new file that has the .VBS extension added. The original files have their attributes set to "hidden." If the worm determines that mIRC (Internet Relay Chat) is installed on the system it will drop a mIRC script that will send the worm on via mIRC. The worm contains a large number of comments inside its code which do not get displayed.

VBS.Nightflight@mm (Visual Basic Script Worm): This is a polymorphic mass mailing worm written in the Visual Basic Scripting (VBS) language. The worm can e-mail itself to all contacts in the Microsoft Outlook Address Book. It can also spread by network drives and it contains functionality such as changing the desktop wallpaper, spreading by mIRC, changing the Windows user information, and lowering security settings on the computer.

VBS/VBSWG-X (Aliases: VBS.HomePage, VBS.VBSWG2.X@mm, VBS.VBSWG2.D@mm, VBS_HomePage.A, VBS/SST.gen@mm) (Visual Basic Script Worm): This virus has been reported in the wild. It is an e-mail aware worm based around the VBSWG virus writing kit. It uses Outlook to e-mail itself to each entry in your Outlook address book. When the worm is executed it saves itself to the file homepage.HTML.vbs in the system temporary directory. The first time it is run the worm sends itself to everyone in your address book and then sets the registry entry "HKCU\software\An\mailed" to 1 to prevent the e-mail code being run multiple times. The worm then randomly chooses one of four possible adult-orientated website addresses and displays it using the default web browser.

VBS/VBSWG-Z (Alias: Mawanella) (Visual Basic Script Worm): This virus has been reported in the wild. It is an e-mail-aware worm. The worm copies itself to a file called Mawanella.vbs in the Windows System directory. It then forwards itself via e-mail to every contact in the Microsoft Outlook address book with the following characteristics:

Subject: Mawanella
Body text: Mawanella is one of the Sri Lanka's Muslim Village
Attached file: Mawanella.vbs

The worm displays a message box saying "Please forward this to everyone." It then displays a window showing a burning house with the text: "Mawanella is one of the Sri Lanka's Muslim Village. This brutal incident happened here 2 Muslim Mosques & 100 Shops are burnt. I hat this incident, What about you? I can destroy your computer I didn't do that because I am a peace-loving citizen."

VBS_YABRAN.A (Aliases: YABRAN.A, VBS.Yabran.A@mm, VBS/Fujimori) (Visual Basic Script Worm): This non-destructive Visual Basic Script (VBS) worm propagates via Microsoft Outlook as an attachment with the name FOTOS_YABRAN_VIVO_HOY.JPG.vbs

VBS_ZEAM.A (Aliases: ZEAM.A, VBS.Zeam.A@mm, VBS/SSIWG2.worm) (Visual Basic Script Worm): This non-destructive Visual Basic Script worm uses Microsoft Outlook to propagate. It sends itself out as an attachment "worm's copy" to all addresses listed in the MS Outlook address book of the infected user. The subject of the e-mail with the worm attachment is "haha."

W32.Excuse.Worm@m (W32 Worm): When W32.Excuse.Worm@m is first executed, it copies itself into the Windows directory as W32_1ST.EXE. Next, XRF \<path>\w32_1st.exe is added to the registry key: HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run. The worm will then retrieve the filename of the Windows Address Book from the registry, choose a random position within the file, and search for an e-mail address that ends in .com.

Win32.HLLW.Showgame (W32 Worm): This is a very dangerous memory resident Win32 virus worm. It doesn't infect files; but spreads "as-is." The 70K Win32 application can be found in three files: in the Windows system directory with WINDOWS.EXE name, in the Windows directory with WINXYZ.EXE name, and on an A: drive with SHOWGAME.EXE name. When the virus is run on an infected floppy disk, it copies itself to the Windows system directory with the WINDOWS.EXE name and to the Windows directory with the WINXYZ.EXE name. The virus then registers itself in the auto-run key in system registry:

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunServices
wwindll = %SystemDir%\winxyz.exe /run"

The virus then stays in the Windows memory as a hidden service process, detects when an A: floppy drive is in use, and copies itself there with the SHOWGAME.EXE name. This file then activates the ReadOnly, System and Hidden attributes. On the 26th of each month, the virus destroys files in the root directory on the C: drive. To destroy files, the virus "creates" them, so a file is not deleted; rather its size is set to zero, and file data is lost. While infecting the system, the virus also modifies the registry key:

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\
Explorer\CabinetState
FullPath = 1

In the Russian Windows version, the virus displays a white ellipse covering the desktop on Saturdays.

Win32.Miam (W32 Worm): This is a dangerous parasitic Win32 virus that infects Win32 PE EXE files (Win32 applications). While infecting, the virus writes its code to the end of the file, and patches the program entry routine with a short code that passes control to the main virus body when an infected file is executed. The virus has bugs and some files can be corrupted during infection. When an infected file is run, the virus looks for Win32 .EXE files in the current directory and infects them. The virus then gets NOTEPAD.EXE and CALC.EXE from the Windows directory and infects them too. Next, the virus hooks the CreateFileA Windows API function and stays memory resident as a hidden sub-process of the host process (infected application). So, the virus is "per-process" memory resident, and is active until an infected application is activated. When any file is being opened, the virus searches for all .EXE files in the current directory and infects them. Depending on the system time (the infected program is run at 10:00 a.m.), the virus drops C:\NEO.BMP, stores an image there and registers that as the Desktop wallpaper. The image has a text on black background:

Wake Up Neo
[win32.Neo]

When the 1st virus generation (virus dropper) is run, it displays the following message:

Win32.Neo Virus by [TiPiaX/VDS]
Miam ! I love PE files ;)

W97M.Hlam.A (Word 97 Macro Virus): When an infected document is closed, the macro virus performs the following actions:

It replicates to the active documents and the Normal.dot template file through the temporary file Fayze.dll that it drops and then deletes.
It looks for the specific executable program appended (not embedded as an OLE stream) to the infected document. Detected as W32.Hlam@mm, this program is used by the macro virus as a "carrier" of the infection.

- If the executable file is found, the macro virus will detach it, drop as Chlam.exe into the same folder, and run it. When executed, the W32.Hlam@mm will copy itself as SysT_eDit.exe into the C:\Windows\System folder.
- If the executable file is not found, the macro virus will open the file SysT_eDit.exe from the C:\Windows\System folder, append it to the end of the infected document, and save the document.

W97M.Hlam.A will change the settings in Microsoft Word to cause the following to occur:

- When you open a document that contains macro, the warning message no longer appears by default.
- When you close Microsoft Word, any changes made to the Normal.dot template are automatically saved without prompting.
- When you save a document, Word saves only changes to a document. When reopening the document, Word uses the saved changes to reconstruct the document.
- When you open a file that is not a Word document or template, the Convert File dialog box does not appear.

W97M.Hlam.A will prevent you from invoking the Visual Basic Editor.

W97M.Tenda.A (Word 97 Macro Virus): This is an encrypted macro virus that infects active documents and the Normal.dot template file. If the day is the 28th of any month, W97M.Tenda.A will attempt to open the following Web site, using the default browser: www.tendadaesperanca.com.br. If the date is March 5, the virus will display a message in Portuguese.

WM97/Bablas-BW (Word 97 Macro Virus): This is a variant of the WM97/Bablas Word macro virus. The virus will change the application caption and the application status bar of Microsoft Word during infection. The text is chosen at random from a selection, but is always similar to "Selamat datang di GRATIA COMPUTER." If the user tries to access the Tools|Macro or File|Templates menu options, the virus displays the message "Untuk keamanan data Anda, fasilitas Macro kami kunci."

WM97/Myna-AB (Word 97 Macro Virus): WM97/Myna-AB is a Word macro virus that does little more than replicate. The replicating code contains the phrase MYNAMEISVIRUS, which is used as a flag to check for its presence.

WM97/Myna-AP (Word 97 Macro Virus): WM97/Myna-AP is a Word macro virus that does little more than replicate. The replicating code contains the phrase MYNAMEISVIRUS, which is used as a flag to check for its presence.

WM97/Replog-D (Word 97 Macro Virus): This a Word macro virus that attempts to run the file I:\Eudora\Sys\Server.exe. It also appends the text 'Active on' and the date to the file I:\Rep.log.

WM97/Thirty4-A (Word 97 Macro Virus): This is a polymorphic Word macro virus. On the 28th of any month the virus attempts to connect to a website in Brazil. On the 5th of March the virus displays a message box containing the text "JOSYE SUA AUTA!!!."

WM97/Thus-EF (Word 97 Macro Virus): This is a Word macro virus. On the 13th or 26th of any month, this virus will display the message "Attention! Do everything, your computer tells you!" when a document is closed. The virus then asks you to enter your name, and displays the message "Do you know, you're the greatest stupid lamer? If no please call WWW.MICROSOFT.COM." On August 13th, or during December, the virus will shut down Windows whenever a document is closed.

XM97/Divi-AB (Excel 97 Macro Virus): This is a variant of the XM97/Divi-A Excel macro virus. It creates a file called BASE5874.XLS in the Excel template directory, and will infect other spreadsheets as they are opened or closed. The virus adds a flag, in the form of a variable called IVID plus a hexadecimal number, to each file as it is infected. The virus uses this flag to determine whether the spreadsheet has already been infected.

XM97/Divi-AH (Excel 97 Macro Virus): This is a variant of the XM97/Divi-A Excel macro virus. The virus creates a viral file called base5874.xls in the XLSTART directory. This file is used during the replication process.

XM97/Laroux-NY (Excel 97 Macro Virus): This is a variant of the XM97/Laroux Excel macro virus. The virus may change the File Properties information to have the following characteristics:

Title: "Fraouk"
Subject: "SIMULATION GEOSTATISTIQUE"
Author: "GEOLOGIE."

The virus creates a file called Vera.xls in the XLSTART directory, which is used during the replication process.

XM97/Pinkpick-A (Excel 97 Macro Virus): This is an Excel macro virus that infects Microsoft Excel spreadsheets. The virus creates a viral file called B00k1.xls that is placed in the XLSTART directory. The virus during its replication process uses this file.

Trojans

Trojan Horse programs have become increasingly popular as a means of obtaining unauthorized access to computer systems. This table starts with Trojans discussed in CyberNotes #2001-01, and items will be added on a cumulative basis. Trojans that are covered in the current issue of CyberNotes are listed in boldface/red. Following this table are descriptions of new Trojans and updated versions discovered in the last two weeks. Readers should contact their anti-virus vendors to obtain specific information on the Trojans and Trojan variants that their anti-virus software detects. *At times, Trojans may contain names or content that may be considered offensive.*

Trojan	Version	CyberNotes Issue #
Backdoor.Acropolis	N/A	CyberNotes-2001-04
Backdoor.Netbus.444051	N/A	CyberNotes-2001-04
Backdoor.NTHack	N/A	CyberNotes-2001-06
Backdoor.Quimera	N/A	CyberNotes-2001-06
Backdoor.SMBRelay	**N/A**	**Current Issue**
Backdoor.WLF	N/A	CyberNotes-2001-08
Backdoor-JZ	N/A	CyberNotes-2001-02
BAT.Install.Trojan	N/A	CyberNotes-2001-04
BAT.Trojan.DeltreeY	N/A	CyberNotes-2001-07
BAT.Trojan.Tally	N/A	CyberNotes-2001-07
BAT_DELWIN.D	N/A	CyberNotes-2001-05
BAT_EXITWIN.A	N/A	CyberNotes-2001-01
BioNet	3.13	CyberNotes-2001-07
BSE Trojan	N/A	CyberNotes-2001-07
DLer20.PWSTEAL	N/A	CyberNotes-2001-05
Eurosol		**Current Issue**
Fatal Connections	2.0	CyberNotes-2001-09
Flor	N/A	CyberNotes-2001-02
Freddy	beta 3	CyberNotes-2001-09
Gift	1.6.13	CyberNotes-2001-09
HardLock.618	N/A	CyberNotes-2001-04
Jammer Killah	**1.2**	**Current Issue**
JS.StartPage	N/A	CyberNotes-2001-07
Noob	4.0	CyberNotes-2001-09
PHP/Sysbat	N/A	CyberNotes-2001-02
PIF_LYS	N/A	CyberNotes-2001-02
PWSteal.Coced240b.Tro	N/A	CyberNotes-2001-04
SadCase.Trojan:	N/A	CyberNotes-2001-09
Scarab	**1.2c**	**Current Issue**
Troj/Futs	N/A	CyberNotes-2001-07
Troj/Keylog-C	N/A	CyberNotes-2001-08
Troj/KillCMOS-E	N/A	CyberNotes-2001-01
Troj/Unite-C	N/A	CyberNotes-2001-09
TROJ_AOL_EPEX	N/A	CyberNotes-2001-01
TROJ_AOLWAR.B	N/A	CyberNotes-2001-01
TROJ_AOLWAR.C	N/A	CyberNotes-2001-01
TROJ_APS.216576	N/A	CyberNotes-2001-03
TROJ_ASIT	N/A	CyberNotes-2001-07
TROJ_AZPR	N/A	CyberNotes-2001-01
TROJ_BADTRANS.A	N/A	CyberNotes-2001-08
TROJ_BAT2EXEC	N/A	CyberNotes-2001-01
TROJ_BKDOOR.GQ	N/A	CyberNotes-2001-01
TROJ_BUSTERS	N/A	CyberNotes-2001-04
TROJ_CAINABEL151	1.51	CyberNotes-2001-06
TROJ_DARKFTP	N/A	CyberNotes-2001-03
TROJ_DUNPWS.CL	N/A	CyberNotes-2001-05
TROJ_DUNPWS.CL	N/A	CyberNotes-2001-04
TROJ_EUTH.152	N/A	CyberNotes-2001-08
TROJ_FIX.36864	N/A	CyberNotes-2001-03
TROJ_FUNNYFILE.A	N/A	CyberNotes-2001-09
TROJ_GLACE.A	N/A	CyberNotes-2001-01
TROJ_GNUTELMAN.A	N/A	CyberNotes-2001-05
TROJ_GOBLIN.A	N/A	CyberNotes-2001-03
TROJ_GTMINESXF.A	N/A	CyberNotes-2001-02
TROJ_HAVOCORE.A	N/A	CyberNotes-2001-09
TROJ_HERMES	N/A	CyberNotes-2001-03

Trojan	Version	CyberNotes Issue #
TROJ_HFN	N/A	CyberNotes-2001-03
TROJ_ICQCRASH	N/A	CyberNotes-2001-02
TROJ_IE_XPLOIT.A	N/A	CyberNotes-2001-08
TROJ_IF	N/A	CyberNotes-2001-05
TROJ_INCOMM16A.S	N/A	CyberNotes-2001-09
TROJ_JOINER.15	N/A	CyberNotes-2001-02
TROJ_JOINER.I	N/A	CyberNotes-2001-08
TROJ_LASTWORD.A	N/A	CyberNotes-2001-09
TROJ_MATCHER.A	N/A	CyberNotes-2001-08
TROJ_MOONPIE	N/A	CyberNotes-2001-04
TROJ_MTX.A.DLL	N/A	CyberNotes-2001-09
TROJ_MYBABYPIC.A	N/A	CyberNotes-2001-05
TROJ_NAKEDWIFE	N/A	CyberNotes-2001-05
TROJ_NARCISSUS.A	N/A	CyberNotes-2001-09
TROJ_NAVIDAD.E	N/A	CyberNotes-2001-01
TROJ_PARODY	N/A	CyberNotes-2001-05
TROJ_PICSHOW.A	**N/A**	**Current Issue**
TROJ_PORTSCAN	N/A	CyberNotes-2001-03
TROJ_Q2001	N/A	CyberNotes-2001-06
TROJ_QZAP.1026	N/A	CyberNotes-2001-01
TROJ_RUNNER.B	N/A	CyberNotes-2001-03
TROJ_RUX.30	N/A	CyberNotes-2001-03
TROJ_SCOUT.A	N/A	CyberNotes-2001-08
TROJ_SUB7.21.E	2.1	CyberNotes-2001-05
TROJ_SUB7.22.D	.22	CyberNotes-2001-06
TROJ_SUB7.401315	N/A	CyberNotes-2001-01
TROJ_SUB7.MUIE	N/A	CyberNotes-2001-01
TROJ_SUB7.V20	2.0	CyberNotes-2001-02
TROJ_SUB722	2.2	CyberNotes-2001-06
TROJ_SUB722_SIN	N/A	CyberNotes-2001-06
TROJ_SUB7DRPR.B	N/A	CyberNotes-2001-01
TROJ_SUB7DRPR.C	N/A	CyberNotes-2001-03
TROJ_TPS	N/A	CyberNotes-2001-05
TROJ_TWEAK	N/A	CyberNotes-2001-02
TROJ_VBSWG_2B	N/A	CyberNotes-2001-07
TROJ_WEBCRACK	N/A	CyberNotes-2001-02
TROJ_WINMITE.10	N/A	CyberNotes-2001-08
Trojan.MircAbuser	N/A	CyberNotes-2001-04
Trojan.PSW.M2.14	N/A	CyberNotes-2001-07
Trojan.RASDialer	N/A	CyberNotes-2001-06
Trojan.Sheehy	N/A	CyberNotes-2001-05
Trojan.Taliban	N/A	CyberNotes-2001-07
Trojan.W32.FireKill	N/A	CyberNotes-2001-07
Trojan/PokeVB5	N/A	CyberNotes-2001-07
VBS.Cute.A	N/A	CyberNotes-2001-05
VBS.Delete.Trojan	N/A	CyberNotes-2001-04
VBS.Lumorg	N/A	CyberNotes-2001-09
VBS.Over.Trojan	**N/A**	**Current Issue**
VBS.Trojan.Noob	N/A	CyberNotes-2001-04
VBS.Zeichen.A	N/A	CyberNotes-2001-08
VBS_HAPTIME.A	N/A	CyberNotes-2001-09
W32.BatmanTroj	N/A	CyberNotes-2001-04
W32.BrainProtect	N/A	CyberNotes-2001-07

Backdoor.SMBRelay: Backdoor.SMBRelay is a backdoor Trojan. It uses the "Man in the Middle" attack, which is a method used for stealing sensitive information from a client to gain access to a server. It uses port 139 (default NetBIOS port) for its malicious activities. It forces a client (the victim) to authenticate

with the attacker. By authenticating with the attacker, the client sends out authenticating information to the attacker as if the client were trying to authenticate with the server. Once the attacker obtains this information, the attacker may use this information to authenticate itself with the server, thus gaining access to the server. It may then disconnect the victim permanently, allowing the connection to be held up by the attacker itself.

Eurosol: This Trojan steals a user's personal account information from the international finance system "WebMoney." The Trojan disguises itself as a CC-Bank program, allegedly allowing for the receiving of money by viewing an advertising module. In order to receive a victim's personal account information from WebMoney, Eurosol locates the file Keys.kwm (a secret key) and Purses.kwm (a virtual "wallet"). In the case of a successful search, the files are encrypted and sent to a remote FTP server. To ensure that the information is successfully transferred, the Trojan neutralizes the installed firewall ATGuard. To complete this, Eurosol modifies its settings so that ATGuard doesn't prevent the installation of the TCP/IP connection with the external servers. After this, the Trojan malefactor is able to obtain the stolen "wallets" and passwords to them from the FTP server, hooking them to the Trojan's WebMoney program copy. The Trojan can then transfer any money contained in the WebMoney account to its own money account, or receive cash via postal transfer in the receiver's name.

Jammer Killah (1.2): Jammer Killah 1.2 is a Trojan that is designed to disable the Jammer program. This program detects Back Orifice and Netbus. Then it drops a Back Orifice 1.20 server. The server is configured on port 121 with password hack.

Scarab (1.2c): Scarab 1.2c is a Visual Basic 4 Trojan. This Trojan has a few unique features, such as changing the server title.

TROJ_PICSHOW.A (Aliases: PICSHOW.A, PICSHOW): This non-destructive, memory-resident Trojan is coded in Visual C++. Upon execution, it displays a message box with the McDonald's icon. At two-minute intervals thereafter, it displays a picture of a girl with ghostly features.

VBS.Over.Trojan (Aliases: VBS.Trojan.Over, Trojan VBS/Over): If the security settings in Internet Explorer are set correctly, then every time that the infected HTML page is opened, the browser will warn you that some software on the page might be unsafe, with the recommendation to not run it. If you allow the software to run, the VBS.Over.Trojan attempts to overwrite the following files:

Win.com
Win.ini
System.ini
User.exe
Rundll.exe
Rundll32.exe
Emm386.exe
Ios.ini
Explorer.exe

When attempting to overwrite these files, VBS.Over.Trojan looks for them only in the folder that is parent to the folder from which VBS.Over.Trojan is running. In most cases, by default, the Trojan runs from the \Windows\Temporary Internet Files folder; this means that \Windows is the parent folder, and most of the target files are located in that folder. In addition, it attempts to rewrite the C:\Command.com file.